CYBERSPACE AS A COMPLEX ADAPTIVE SYSTEM AND THE POLICY AND OPERTIONAL IMPLICATIONS FOR CYBER WARFARE

A Monograph

by

Major Albert O. Olagbemiro

United States Air Force

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

AY 2014-001

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
22-05-2014	Master's Thesis	JUL 2013 - MAY 2014

4. TITLE AND SUBTITLE

CYBERSPACE AS A COMPLEX ADAPTIVE SYSTEM AND THE POLICY AND OPERTIONAL IMPLICATIONS FOR CYBER WARFARE

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

ALBERT O. OLAGBEMIRO
Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The overall implication of depicting cyberspace as a complex, adaptive ecosystem is that it provides an avenue for further insight and understanding of the complexities associated with operating in cyberspace. This renewed reality highlights a source of vulnerability, a potential threat to national security, due to the intermixing of public and private infrastructure and the reliance of the United States Government (USG) on infrastructure owned and operated by the private sector. The fact that most, if not all, of the underlying infrastructure for seamless cyber interactions are controlled and managed by non-state entities means that the USG most recognize the power of the private sector in cyberspace. This represents a disturber of the familiar international order because the major actor that constitutes and defines international relations (the state) is not able to control cyberspace or to insulate itself from the implications of the new cyber realities. This recognition suggests that adopting a policy position that is primarily offensive in nature better serves the US, especially in regards to the protection of the cyber ecosystems of the private sector.

15. SUBJECT TERMS

Complex Adaptive System, Cyberspace, Infosphere, Cyber Warfare, Cyber Ecosystem

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
Unclassified	Unclassified	Unclassified	UU	47	

MONOGRAPH APPROVAL

Name of Candidate: Major Albert O. Olagbemiro

Monograph Title: Cyberspace as a Complex Adaptive System and the Policy and Operational Implications for Cyber Warfare

Approved by:

_____, Monograph Director
Jeffrey J. Kubiak, Ph.D.

_____, Seminar Leader
Charles M. Evan, COL, FA

_____, Director, School of Advanced Military Studies
Henry A. Arnold III, COL, IN

Accepted this 22nd day of May 2014 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

ABSTRACT

CYBERSPACE AS A COMPLEX ADAPTIVE SYSTEM AND THE POLICY AND OPERATIONAL IMPLICATIONS FOR CYBER WARFARE, by Major Albert O. Olagbemiro, USAF, 47 pages.

The overall implication of depicting cyberspace as a complex, adaptive ecosystem is that it provides an avenue for further insight and understanding of the complexities associated with operating in cyberspace. This renewed reality highlights a source of vulnerability, a potential threat to national security, due to the intermixing of public and private infrastructure and the reliance of the United States Government (USG) on infrastructure owned and operated by the private sector. The fact that most, if not all, of the underlying infrastructure for seamless cyber interactions are controlled and managed by non-state entities means that the USG most recognize the power of the private sector in cyberspace. This represents a disturber of the familiar international order because the major actor that constitutes and defines international relations (the state) is not able to control cyberspace or to insulate itself from the implications of the new cyber realities. This recognition suggests that adopting a policy position that is primarily offensive in nature better serves the US, especially in regards to the protection of the cyber ecosystems of the private sector. Specifically it proposes that offensive cyber attacks should not be limited to only the authorized entities of the United States military, but should be expanded to include authorized entities in the private sector. Central to this proposition is the introduction of a new element of operational art specific to the cyber realm to guard against unintended consequences—the operational art element of precision.

TABLE OF CONTENTS

ACRONYMS

ARPAnet	Advanced Research Projects Agency network
CARL	Combined Arms Research Library
CAS	Complex Adaptive System
CGSC	U.S. Army Command and General Staff College
CW	Cyber Warfare
DOD	Department of Defense
EMR	Electromagnetic Radiation
EMS	Electromagnetic Spectrum
EW	Electronic Warfare
MMAS	Master of Military Art and Science
MR	Military Revolution
RMA	Revolution in Military Affairs
SAMS	School of Advanced Military Studies
SeE	Socio Ecological Ecosystem
US	United States
USG	United States Government

ILLUSTRATIONS

> In the information-communication civilization of the 21st Century, creativity and mental excellence will become the ethical norm. The world will be too dynamic, complex, and diversified, too cross-linked by the global immediacies of modern (quantum) communication, for stability of thought or dependability of behavior to be successful.
>
> —Timothy Leary, *Chaos & Cyber Culture*

INTRODUCTION

Actors across all levels of society use cyberspace with each actor having different roles, motivations, and intentions. Associated complexities of safeguarding cyberspace contribute to the lack of a United States (US) policy for operating in cyberspace. This conceptual disorder stems from the current definition of cyberspace which fails to acknowledge the human dimension of cyberspace and the multiplicity of variables resulting in emergent properties, which arise due to the co-mingling of both public and private sector actors in cyberspace. The result is a form of social entropy in which social distinctions between state and non-state actors all but disappears, leading to a situation of jurisdictional arbitrage in which both state and non-state actors are able to exploit the relative anonymity in which cyberspace confers during cyber operations.[1]

The current situation requires a paradigm shift that rejects the prevailing conventional science and embraces a revolutionary approach.[2] This transition from conventional to a revolutionary science requires a new theory of the phenomenon of cyberspace. This new theory suggests that cyberspace is not a domain, but is rather a *socio-ecological ecosystem*—an instance of a dynamic complex adaptive system. This socio-ecological ecosystem exists within a much larger information environment, known as the infosphere. It is this infosphere that constitutes the domain and not cyberspace. As the domain, the infosphere serves as the overall universe of physical and cognitive communication processes.

---

[1]Nir Kshetri, "Pattern of Global Cyber War and Crime: A Conceptual Framework," *Journal of International Management* 11, no. 4 (December 2005): 541-62, doi:10.1016/j.intman.2005.09.009 (accessed 7 February 2014).

[2]Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 4th ed. (Chicago: The University of Chicago Press, 2012), 5-6.

By conceiving cyberspace as a socio-ecological ecosystem, the critical importance of the civilian private sector further emerges due to the reliance of United States Government (USG) entities on a cyber infrastructure predominantly owned and operated by organizations in the civilian private sector. The implications of this revisionist approach leads to a theory of action, which suggests the concept of mutually assured cyber deterrence offers limited operational utility in the cyber realm. The new paradigm suggests the USG is better served by adopting the theory of action more offense-minded as the cornerstone of its policy. Key to the successful adoption of this policy is the introduction of the new operational art element of *precision* that is specific to the cyber realm. It emerges as an operational art element because of the need to guard against unintended consequences associated with offensive cyber attacks.

Research Question and Design

The focus of this monograph is, therefore, to answer the following question. Given the current lack of a USG policy, can the tenets of complexity theory provide a roadmap for operating in cyberspace? The context supporting this line of inquiry are cyber-attacks against US private and public sector entities, to include the US Department of Defense (DOD), during nominal peacetime conditions in other than formally declared acts of war. Any findings along this line of inquiry could potentially have significant operational implications for the USG. The findings would help shape development of a USG policy for operating in cyberspace, from which an overt policy for the DOD and private sector policy could be deduced.

The objective of this research is to seek a US operational strategy for operating in cyberspace. Achieving the stated research objective requires a three-step process. The first step involves bringing coherence to current reasoning in the state of the art by developing a broad, ontological taxonomy of cyberspace. With this step comes a suggested paradigm shift, which is critically important given the proliferation of competing viewpoints and terminology surrounding cyberspace. Thus, the structure of knowledge as pertains to its current depiction needs to be

reconciled. The argumentation in this step points to the idea that the current DOD definition of cyberspace, which largely shapes current US narrative and permeates the public sphere, is flawed. The output of this step is a new theory of the phenomenon of cyberspace. The next step seeks to answer the core research question by building on the new theory of the phenomenon of cyberspace. This step proposes a theory of action, an operational theory for operating in cyberspace based on the renewed conceptualization of cyberspace. Finally, the monograph discusses the implication of this new theory.

SEEDS OF COMPLEXITY

The term cyberspace is fundamentally an abstraction. As an abstraction, it manifests itself into physical reality through the Internet. The physical manifestation of cyberspace is necessary because it needs an underlying means to exist in the physical realm—a mechanism, which the Internet provides in the form of a worldwide, publicly accessible series of, interconnected computer networks. The concept of *open architecture networking* was central to the design of the Internet with the idea of individual networks, independent of each other, possessing and presenting their own unique interface for integration, thereby creating a *network of networks*.

While the concept of open-architecture networking is the most powerful feature of the Internet, it is, however, also its weakness as anyone can connect to the Internet without constraints on the types or geographic scope of networks. This open-architecture networking concept makes it simple for hostile cyber participants to connect to the Internet. Furthermore, communication within this *network of networks* is primarily enabled by commercial entities through multiple interconnected backbones, called “Tier 1” providers who provide the underlying infrastructure (e.g., routers, switches, etc.) through which data is transmitted.

As it currently stands, these Tier 1 providers carry up to 98 percent of all USG communication traffic.[3] One aspect of the complexity associated with operating in cyberspace stems from the USG reliance upon a physical infrastructure controlled and managed by non-state entities—the civilian private sector. This near-complete intermixing of civilian and government computer infrastructure, therefore, makes civilian infrastructure and civilian providers legitimate targets under the law of armed conflict.[4] Further complicating the situation is the unintended consequences that can arise during a cyber attack due to co-mingling of USG and civilian actors. Hence, the central challenge of operating in cyberspace arises because an attacker can never be 100 percent certain that the action will affect only the intended target.

US Response

To address the complexity associated with operating in cyberspace, the Bush Administration rolled out its first public strategy document, *National Strategy to Secure Cyberspace,* in 2003. This document correctly acknowledged the transversal nature of cyberspace, and outlined a strategy hinged on public-private partnership efforts. The Joint Chiefs of Staff (JCS) published the *National Military Strategy of the United States of America (NMS)* and the *National Military Strategy for Cyberspace Operations (NMS-CO*) in 2004 and 2006 respectively. Of note, the 2004 NMS included the term "cyberspace" for the first time as one of the domains of the battle space along with air, land, sea, and space. The 2006 NMS-CO took things a step further by focusing specifically on the characterization of this cyberspace domain, and proposed a strategic military framework to ensure US military superiority in cyberspace.[5]

---

[3]Eric Jensen, "Cyber Warfare and Precautions against the Effects of Attacks," *Texas Law Review* 88 (1 June 2010), http://ssrn.com/abstract=1661218 (accessed 3 March 2014).

[4]Ibid.

[5]US Department of Defense, *The National Military Strategy For Cyberspace Operations* (Washington, DC: 2006), 1-54.

In 2011, DOD released its *Strategy for Operating in Cyberspace*. This document came on the heels of the Obama Administration's *International Strategy for Cyberspace*, also published 2011. Taking into consideration several strategic themes, the Obama strategy document noted that the development of norms for state conduct in cyberspace did not require a reinvention of customary international law, nor did it render existing international norms obsolete.[6] The 2011 DOD strategy further complemented the Obama strategy document, which called for the enhancement of the United States Military's capabilities by outlining a list of initiatives associated with the establishment of cyberspace as an operational domain.[7]

At the core of both these documents was the notion of developing and enhancing existing alliances to strengthen collective cyber security. The documents argued that the development of internationally shared situational awareness and warning capabilities would enable collective self-defense and collective deterrence.[8] However, the limitations of such an alliance-based approach are best exemplified by the limited success of the Budapest Cybercrime Convention, which despite its existence for over ten years, has been ratified by only forty-one nations out of more than 190 countries worldwide.[9]

Furthermore, recent allegations leveled against the United States of alleged cyber surveillance and collection by its National Security Agency (NSA) could potentially hinder any meaningful form of large-scale international cooperation in the cyberspace. Such allegations, while not constituting a new paradigm, serve to reaffirm the existing reality that, "allies spy on allies," and it all comes down to self-interest. A friend today may not be one tomorrow.

---

[6]Office of the President of the United States of America, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: 2011), 1-30.

[7]US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: 2011), 1-19.

[8]Ibid.

[9]"Convention On Cybercrime CETS No.: 185," Council of Europe, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (accessed 13 February 2014).

Therefore, the effectiveness of any alliance-based strategy remains dubious, especially one in which the United States might play a dominant role, as potential allies would be inclined to cooperate meaningfully only to the extent that the cooperation serves mutual interests.

While selected bi-laterally negotiated agreements could potentially offer a pathway for large-scale international cooperation, the reality is the United States may have to occasionally resort to tacit approaches without explicit agreement of the international community.[10] Alternatively, the United States can also impose cooperation. Under this alternative, the United States, as the stronger party, and possibly the party with the most to lose in cyberspace, could force its allies in the international community to alter their policies. The problem with this approach, however, is the United States does not currently have a domestic policy regarding cyberspace. This is because the definition of cyberspace, as currently proposed, is self-limiting. Thus, a new conceptualization of cyberspace is required.

Strategic Discourse

The perception that cyberspace is a domain where fighting takes place and requires domination, pervades the United States military thinking on the subject of cyber war.[11] As of 2014, DOD defined cyberspace as:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[12]

---

[10]Helen Milner, "International Theories of Cooperation among Nations Cooperation among Nations" by Joseph Grieco; Saving the Mediterranean by Peter Haas: Strengths and Weaknesses," *World Politics* 44, no. 3 (April 1992): 96, 466.

[11]Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), 26.

[12]US Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: US Government Printing Office, 8 November 2010), 64.

This definition is correct in that it correctly acknowledges the existence of cyberspace within the information environment. It falls short because it is void of the social contextual factors of today's prevailing reality. Essentially the definition represents a failure to correctly recognize cyberspace for the Military Revolution (MR) that it is. The tendency is to characterize cyberspace primarily as a Revolution of Military Affairs (RMA) without recognizing its contextual relationship with civil society. This distinction is critically important because MRs and RMA are two separate, but related concepts that are not interchangeable.

It is how one conceptualizes MRs and distinguishes it from RMA that forms the core of the debate.[13] Key to understanding the relationship between MRs and RMA is the recognition that MR represents a larger revolution, made up of smaller RMAs.[14]The characteristics of RMA are such that it involves major changes in the nature of warfare brought about by advances in military technology, which combined with dramatic changes in doctrine and organizational concepts, fundamentally alter the character and conduct of military operations.[15] A MR on the other hand is the product of different forces, and includes a social wave characterized by an outgrowth of changes in economic production—the way humans make war reflects the way they make wealth.[16] In the current social wave—the Information Age—information is the key source of wealth and power. This reality leads to a new kind of war in which information is the new

[13]Michael Thompson, "Military Revolutions and Revolutions in Military Affairs: Accurate Descriptions of Change or Intellectual Constructs?" 83 -108, http://artsites.uottawa.ca/strata/doc/strata3_082-108.pdf (accessed 29 March 2014).

[14]Ibid., 95.

[15]Elinor Sloan, "Canada and the Revolution in Military Affairs: Current Response and Future Opportunities," *Canadian Military Journal* (Autumn 2000): 7, http://www.journal.forces.gc.ca/vo1/no3/doc/7-14-eng.pdf (accessed 30 March 2014).

[16]Thompson, 93.

strategic asset, and control of information will not only be the *ends* of war, but the *means* of war.[17]

Consequently, there are two different narratives for classifying cyberspace. The first narrative suggests that if the United States is indeed facing a MR (i.e., the Information Age represents a MR), then the United States policy debate should transcend issues of technology and operations from a political, economic, and social perspective, and include the fundamental aspects of defense policy.[18] On the other hand, the second narrative suggests that if we are facing an RMA, then the challenge is manageable within the current DOD framework, so long as it maintains the ability to innovate.[19] However, cyberspace is a MR, and because a MR is a product of deep, varied social forces, it is less controllable and often beyond the control of DOD future-oriented or strategic thinkers.[20] It is apparent that DOD has de-linked cyberspace from the broader MR. DOD continues to treat cyberspace solely as a RMA because it allows DOD to retain control, as RMAs are generally susceptible to institutional direction.

The problem, however, is that by treating cyberspace as an independent RMA, DOD has largely ignored the fact that virtually all of the USG public sector, to include DOD, relies on an underlying infrastructure owned and operated by the private sector. It also ignores the amount of social activity, especially commerce, which takes place in cyberspace. By ignoring the political, economic, and social impacts of cyberspace attributable to civil society, it appears DOD has essentially defaulted to a position that technology is an underlying factor and cause of a MR. However, technology is an underlying factor, but not necessarily the cause of a MR.

---

[17]Thompson, 93.

[18]Ibid., 96.

[19]Ibid.

[20]Ibid.

This is why the current characterization of cyberspace as a domain is flawed. It focuses solely on the technical aspects of cyberspace and fails to acknowledge the importance of the human actor. This subtle, but important observation has severe operational consequences and contributes to the current discourse surrounding the development of a US policy for operating cyberspace. As the institution largely responsible for pioneering the use of cyberspace, the epistemology as developed by DOD plays a huge role in shaping US discourse on the topic.

THE THEORY OF THE PHENOMENON: REDEFINING CYBERSPACE

There is a need to provide a revised definition of cyberspace to help refocus the debate. This new definition must acknowledge and incorporate the role of the human actor. Key to this new conceptualization is the notion that cyberspace consists of three primary dimensions. Each of these dimensions represents a logical grouping of the primary actors (someone or something, which has a capacity to interact) in cyberspace; these are the *human*, *application*, and *infrastructure* dimensions. Collectively, these dimensions make up the *cyber triad*. Figure 1 below, provides a depiction of this notional cyber triad.

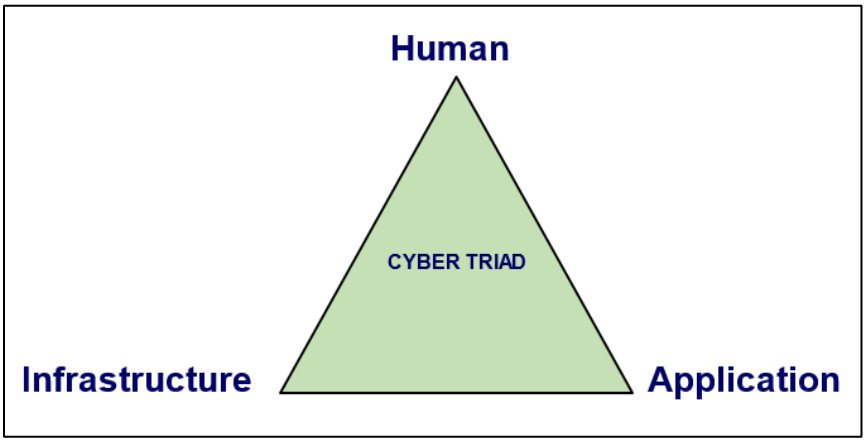

Figure 1. Cyber Triad.

Source: Created by author.

This cyber triad represents a system of regularly interacting and interdependent dimensions forming a unified whole in the broader universe of information. The application dimension represents the underlying software applications (e.g., operating systems, computer applications, etc.) which computers run on or use to deliver value to an end user. The infrastructure dimension constitutes the mediums, platforms, and hardware devices through which data storage, transfer, and communication occurs. The human dimension represents the human actor and its role in consuming and or contributing value in the cyber triad, and includes all users of cyberspace, as well as the engineers and researchers who contribute to the development of the application and infrastructure dimensions of the cyber triad.

Of particular importance in this new conceptualization is the implicit recognition that the cyber triad exists within the context of an information environment known as the *infosphere*. This infosphere constitutes the broader domain rather than cyberspace itself. Cyberspace does not constitute the domain because it is a man-made environment used to exploit other domains. At its core, it is merely a digital environment that is ubiquitous in nature. This begets the question—if cyberspace is not the domain, what is cyberspace? This monograph argues that cyberspace is an ecosystem, a complex adaptive system to be precise, which exists within an environment known as the infosphere. This perspective represents a crucial point of departure from conventional thinking because the conceptualization of cyberspace as an ecosystem within the infosphere fully illuminates the complementary role in which cyberspace plays with other information-centric forms of war such as electronic warfare within the broader spectrum of information operations.

Key to this line of departure is a recognition that cyberspace operations are fundamentally conducted to influence decisions or the decision-making process, be it a machine or the human decision maker, through the manipulation of ones and zeroes. The development of the requisite ontology surrounding cyberspace requires the acknowledgment of the importance of the human dimension as well as the understanding that cyberspace is an open-system—a key trait

of a complex adaptive system. Since it is as an open-system, it would interact with other entities within the infosphere, which implies that classical systems theory could offer some utility towards the development of an operational theory for operating in cyberspace. The pursuit of this line of inquiry requires the exploration of concepts native to the field of classical systems theory. In this regard, the field of biological ecology provides an avenue to further illustrate the applicability of classical systems theory to the cyber triad.

Cyberspace as an Ecosystem

By definition, an ecosystem (short for *ecological system*) is a community and its physical environment treated together as a functional system.[21] From a biological perspective, this community consists of the living (biotic) organisms (e.g., plants, animals, and microbes) and the non-living (abiotic) environment in which the living organisms exist (e.g., air, water, mineral soil).[22] The ultimate goal of the biotic agents in a biological ecosystem is survivability or sustainability. In a biological ecosystem, the accomplishment of this goal is dependent on three key processes.

The first of these processes concerns the flow of energy, and how it enters an ecosystem.[23] This is a critical process because energy is the most essential requirement of all living organisms in a biological ecosystem.[24] The second process focuses on the trophic (feeding) structure in order to understand the cycle of materials *within* an ecosystem. The trophic structure is a hierarchical classification of the organisms in a given ecosystem. The hierarchical structure is primarily dependent on the energy source that an organism relies upon, and how the organism

[21]F. Stuart Chapin, P. A. Matson, and Harold A. Mooney, *Principles of Terrestrial Ecosystem Ecology* (New York: Springer, 2002).

[22]Ibid.

[23]"Environmental Biology—Ecosystems," http://www.marietta.edu/~biol/102/ecosystem.html#Energyflowthroughtheecosystem3 (accessed 14 February 2014).

[24]Ibid.

provides energy for other organisms in the food web. Essentially, this is an interlocking series of "who" eats "whom," commonly called a food chain. [25] Abiotic factors also play an important role in this food chain because climate will decide which food resources, and how much water and sunlight are available to organisms in any given environment.[26] The third process focuses on the emergent behavior, which arises due to changes occurring in the ecosystem.

Similar to a biological ecosystem, the cyber triad is a community and its physical environment interacting together as a functional system. In this case, the cyber triad constitutes the ecosystem. This ecosystem is the *cyber-ecosystem*. The human dimension denotes the biotic component, while the infrastructure and application dimensions denote the abiotic components in the cyber-ecosystem. The desired goal of the biotic component in the cyber ecosystem is survivability. Survivability is the ability of the cyber ecosystem to function continually during and after a *disturbance.*[27] It requires the biotic component to maintain a position of continuing advantage given the disturbances introduced by competing social, political and economic factors in cyberspace.

The first biological process (energy flow) occurs when energy from the sun enters a biological ecosystem. This energy *enters* the ecosystem as solar radiation. Therefore, solar energy serves as the key energy source, which sustains the continuous cycle of life in a biological ecosystem. The requirement for energy flow process is conceptually satisfied in a cyber ecosystem through an organization's intellectual capital—knowledge. Intellectual capital is the

[25]Environmental Biology–Ecosystems."

[26]"Food Web Background," http://www.seagrant.sunysb.edu/ifishny/pdfs/lessons/inclass/elementary/FoodWeb-Background.pdf (accessed 3 April 2014).

[27]C. A. Kamhoua and K. A. Kwia, "Survivability in Cyberspace Using Diverse Replicas: A Game-Theoretic Approach," *Journal of Information Warfare* 12, no. 2 (23 July 2013), http://www.jinfowar.com/survivability-in-cyberspace-using-diverse-replicas-a-game-theoretic-approach/ (accessed 3 April 2014).

most essential requirement of the biotic actor, and it is the key energy flow required to sustain the cycle of competiveness in the cyber ecosystem. Without it, the cyber ecosystem ceases to exist.

The intellectual capital of a cyber ecosystem is knowledge and it includes all non-monetary and non-physical resources that contribute to the value creation of the cyber ecosystem.[28] Intellectual capital includes the ability to understand the changing nature of technology as well as the continuous evolution of the cyber environment. Not only is intellectual capital the key source of energy for the cyber ecosystem, it is also the only material which is manifested and cycled within an ecosystem in the form of technical expertise. This technical know-how in turn translates into securing or improving one's position of relative advantage in the infosphere.

Just like the biological ecosystem, the cyber ecosystem also has a trophic (feeding) structure (second biological process). A rather simplistic illustration of the trophic structure is a scenario in which the human actor, as the sole biotic actor in the cyber ecosystem, consumes information created by an application in the application dimension. An application in the application dimensions, in turn, consumes resources (e.g., processors) in the infrastructure dimension. This rather simplistic scenario of a cyber trophic structure does not imply there is only one order possible from any producer to any one ultimate consumer. Rather it infers that in any given cyber trophic structure, a complex structure consisting of a web of interactions could arise. Besides being an open system, any given cyber ecosystem is not a unitary entity in an infosphere; i.e., there are several cyber ecosystems within the infosphere. It is rather the fundamental structure of all cyber ecosystems within the larger infosphere. Therefore, it is possible to talk about primary consumers, secondary consumers, and even tertiary and quaternary consumers when trying to understand the chain of interaction between each of the dimensions in the cyber

[28]Adapted from Eckhard Ammann, "A Hierarchical Modelling Approach to Intellectual Capital Development," *The Electronic Journal of Knowledge Management* 8, no. 2: 182-183.

ecosystem.[29] Similar to a biological ecosystem, given this complex web of interactions in cyberspace, complexity begins to arise.

The third pertinent biological process (change process) is also a requirement for survivability because the biological ecosystem must adapt to changes in both the biotic and abiotic factors. This need for adaptation also gives rise to complexity because of the multiplicity of interactions due to the trophic structure, which then introduces emergence into the ecosystem. The introduction of emergent properties is such that the ecosystem assumes a new pattern of behavior or structure, which more often than not is either unexplainable or unpredictable even when the individual organisms in the ecosystem are studied.

The ability of the cyber ecosystem to change and adapt to changing conditions becomes a requirement for continued survivability. Emergence arises in the cyber ecosystem due to the varying forms of perturbations or feedback within the ecosystem. When an ecosystem is subject to any sort of perturbation, it responds by moving away from its initial state to a new adapted state.[30] From a cyber perspective, this translates into a cyber ecosystem's ability to adapt to emergent conditions in order for it to continue to be a viable medium during cyber operations. Of particular importance in this logic is the recognition that the need for adaptation is not constrained to the actors in the human dimension (cyber operator) alone. Actors in both the application and infrastructure dimensions, when purposely designed, are also capable of self-adaptation to handle changing conditions such as system intrusions. Thus, the need for adaptation further puts a cyber ecosystem into a new category of ecosystems. This is the category of dynamical ecosystems. This

[29]Michele Nash and Lisa Rapp, "Trophic," Springfield Technical Community College, http://faculty.stcc.edu/biol102/Lectures/lesson12/trophicstruc.htm (accessed 14 February 2014).

[30]"Building a Dynamic Financial Ecosystem," *New Straits Times*, 21 November 2012, http://www.nst.com.my/opinion/columnist/building-a-dynamic-financial-ecosystem-1.174254 (accessed 14 February 2014).

further leads to the conceptualization of the cyber ecosystem as being a dynamic, complex adaptive system.

Role of the Infosphere

Any action within the infosphere is fundamentally an information operation, and cyber operations (activities conducted in cyberspace) represent just one type of an information operation. The idea of the existence of a "virtual space" out there, connected to, but often removed from real physical spaces provides the basis for conceiving cyberspace as an ecosystem.[31] The infosphere is the virtual space, which serves as the overall universe of physical and cognitive communication processes. It encompasses all aspects of information centric operations ranging from electronic warfare to psychological operations. The infosphere is also the entity that DOD doctrine refers to as the *information environment* in which humans and automated systems observe, orient, decide, and act upon information.[32]

Native to the infosphere is a form of energy known as electromagnetic radiation (EMR), which enables wireless communications. The propagation of EMR occurs through electromagnetic waves with the full range of frequencies ranging from radio waves, gamma rays, and visible light, all constituting the electromagnetic spectrum (EMS).

When it comes to the world of wireless communications, the waveforms beneath visible light enable wireless transmissions beyond direct point-to-point connections. As the key enabler of wireless communication in the infosphere, the EMS has a symbiotic relationship with cyberspace because cyberspace routinely requires wireless in addition to wired links to transport information. Since cyberspace operations require the use of the EMS for enabling full effects in

[31]Adapted from Stephen D. McDowell, Philip E. Steinberg, and Tami K. Tomasello, *Managing the Infosphere: Governance, Technology, and Cultural Practice in Motion* (Philadelphia: Temple University Press: 2008), 10.

[32]US Department of Defense, Joint Publication 3-13: *Information Operations* (Washington, DC: 2010).

cyberspace, viewing the cyber ecosystem as an open-system encapsulated by the infosphere in which EMR facilitates wireless interactions offers greater utility in the current discourse for two key reasons.

First, it highlights the problems with characterizing cyberspace as a domain. The core objective of warfare in any given domain is to achieve a degree of control within the domain. This objective gives rise to terms such as air, maritime, space and land superiority, which reflect duration-specific command of the respective domains. If cyberspace is treated as a domain, then it is possible to generate the concept of cyber superiority. The problem is that the idea of cyber superiority shifts the focus away from the larger objectives sought by operating in cyberspace. In this regard, cyberspace should be viewed as a capability within the broader infosphere domain in which information operations are conducted. Operating in cyberspace should not be the *ends* in itself, but rather a *means* and *ways* within the context of the larger information environment. Thus, just as Douhet and Corbett emphasized the need to establish command of the air and sea domains respectively in order to achieve military objectives, so must one seek command of the infosphere to achieve the desired objectives.

The second reason why this view offers greater utility in the current discourse is that it lays to rest the question surrounding the issue of sovereignty in cyberspace. When one constructs the cyber-triad as an open-system within the infosphere, the notion of sovereignty in cyberspace collapses because open-systems do not respect state boundaries.[33] This conflicts with current interpretations of the concept of sovereignty, which provides the fundamental basis of the current international order that hinges on the notion of supreme dominion, authority, or rule by a nation

[33]Adapted from K. Conca, "Rethinking the Ecology-Sovereignty Debate," *Millennium - Journal of International Studies* 23, no. 3 (March 1994): 701-11, doi:10.1177/03058298940230030201 (accessed 14 February 2014).

state.[34] Attempts to exercise national decision-making, adjudication, and authority do not coincide with the fundamental ecological realities of an open-system, leading to the frustration of any attempts to exercise sovereignty in cyberspace, however the state will continue to play an important role in cyberspace.[35]Furthermore, it is the very belief that cyberspace should be free from government interference or sovereignty, which led to the very idea of cyberspace in the first place.[36] Emphasis should be on the development of an understanding of the interactions between the dimensions of the cyber triad and its surrounding environment.

The Cyber Ecosystem as a Complex Adaptive System

There is no concise, universal definition of a complex system to which everyone ascribes.[37] However, the phenomenological definition is that it exhibits nonlinear, emergent, adaptive behavior.[38] In cyberspace, this definition translates into the complex interconnections and inter-relationships between the dimensions of a cyber ecosystem. Complexity only emerges when the openness of the cyber ecosystem in relation to the infosphere is taken into consideration, and the interactions between the dimensions of a given ecosystem are examined from the perspective of both its internal dynamics as well as its relationship with the infosphere.

This perspective is crucial because, in order to fully understand how a dynamic system evolves over time, all possible variables must be accounted for to determine how it is adapting or responding to the changes. This holistic approach advances the viewpoint that a cyber ecosystem

---

[34]Lieutenant Colonel Patrick W. Franzese, "Sovereignty in Cyberspace: Can It Exist?" *The Air Force Law Review, AFPAM 51-106* 64 (2009): 8.

[35]Adapted from Conca. "Rethinking the Ecology-Sovereignty Debate."

[36]Franzese, *Sovereignty*, 11.

[37]James Ladyman, James Lambert, and Karoline Wisener, "What Is a Complex System?" 1, http://philsci-archive.pitt.edu/9044/4/LLWultimate.pdf (accessed 14 February 2014).

[38]James Moffat, *Complexity Theory and Network Centric Warfare*, Information Age Transformation Series (Washington, DC: CCRP Publication Series, 2003), 51.

is a special instance of a complex system, which is a Complex Adaptive Ecosystem—a concept synonymous with a Complex Adaptive System (CAS). A CAS is a dynamic system able to adapt and evolve with a changing environment. By acknowledging the human dimension, cyberspace becomes a coherent system of biophysical and social factors that regularly interact in a resilient, sustained manner.[39] Key to this realization is the understanding that the structure and behavior of the cyber ecosystem changes over time in a way which *tends* to increase or decrease its success.[40] Due to the changes in the structure and behavior of the cyber ecosystem, two key issues arise. These issues center on the cognitive complexities associated with developing cyber awareness and cyber understanding.[41]

Cyber awareness focuses on the *what*, *where*, and *when* questions.[42] These awareness related questions are in relation to the operational situation as exists at a given moment in time, current or past.[43] These questions essentially help determine "what is going on or what happened" in a cyber ecosystem. Cyber understanding, on the other hand, is essentially the process of making sense of the available information by focusing on the *why* and *who* questions, and drawing inferences about possible consequences of the operational situation.[44] Key to the difference between these two concepts is where cyber awareness deals with the operational environment, as it "was," cyber understanding deals with the operational environment as it is

---

[39]C. L. Redman, M. J. Grove and L. Kuby, "Integrating Social Science into the Long Term Ecological Research (LTER) Network: Social Dimensions of Ecological Change and Ecological Dimensions of Social Change," *Ecosystems* Vol.7 (2) (2004): 161-171.

[40]Paul Phister, "Cyberspace: The Ultimate Complex Adaptive System," *The International C2 Journal* 4, no. 2 (2010–2011), 1-19, http://www.DODccrp.org/files/IC2J_v4n2_03_Phister.pdf (accessed 14 February 2014).

[41]Ibid.

[42]Ibid.

[43]Ibid.

[44]Ibid.

becoming.[45] The goal of cyber understanding is to understand adversarial intentions or to make sense out of seemingly disparate actions/information gleaned through cyber awareness.[46]

The development of cyber awareness and cyber understanding hinge on the ability to detect intruders and anomalous conditions. Cyber understanding also hinges on the ability to analyze and correlate the information garnered from the observations to understand attack sources and intent, in order to respond to the threat. Cyber awareness and understanding remain critically important, and can only be tackled when there is an inherent recognition that cyberspace is a complex adaptive system.

Since the human dimension is a key component, cyberspace as CAS in a broader infosphere is essentially a *socio-ecological ecosystem* (SeE). With this recognition comes the acknowledgment that the traditional properties of a CAS are directly applicable in cyberspace operations. These are the properties of nonlinearity, emergent behavior, and the interplay between chaos and non-chaos. It is the understanding of the impacts of these properties that provide the basis for the development of a theory of action for operating in cyberspace.

[45]Phister, "Cyberspace: The Ultimate Complex Adaptive System."

[46]Ibid.

THEORY OF ACTION: PREDICTABILITY IN CYBERSPACE OPERATIONS

In the varied theories on non-linear complex systems, uncertainty and surprise is not the exception, but the rule.[47] This is due to the feedback effect—a critical attribute of non-linear complex adaptive systems. The notion of the cyber ecosystem as being a SeE is to emphasize the integrated concept of humans in cyberspace, and to stress that the delineation between social systems and ecological systems is artificial and arbitrary.[48] Supporting this viewpoint is the notion that as a SeE, feedback mechanisms link the social ecological aspects of a cyber ecosystem.[49]

In this SeE, learning occurs during normal, cooperative interaction between actors as well as during a cyber conflict between belligerents with the resulting adaptation in response to the learning being dependent on feedback. Therefore, the feedback effect is a means of "communication" through which actors within any of the dimensions of the ecosystem receives information back from its environment about its actions. As the actors within each of the dimensions of the cyber ecosystem interact, the results of some interactions may influence future interactions. This influence represents the feedback within the cyber ecosystem.

The dynamics of a given conflict are based on the interactions rather than the individual actions of actors. In this regard, two types of feedback effects characterize the interactions: positive and negative. Positive feedback influences the interactions between the dimensions in a cyber ecosystem by building on previous actions with a resulting effect being that uninhibited positive feedback can lead to exponential rates of growth in output and a cyber ecosystem

---

[47]Marion Glaser et al., "Human / Nature Interaction in the Anthropocene Potential of Social-Ecological Systems Analysis, 77," http://www.dg-humanoekologie.de/pdf/DGH-Mitteilungen/GAIA200801_77_80.pdf (accessed 30 March 2014)

[48]Ibid.

[49] Fikret Berkes, Johan Colding, and Carl Folke, eds., *Navigating Social-Ecological Systems: Building Resilience for Complexity and Change* (Cambridge: Cambridge University Press, 2003), 3, accessed 10 April 2014, http://0-dx.doi.org.oasis.unisa.ac.za/10.1017/cbo9780511541957.

"exploding" into chaotic behavior.[50] Negative feedback on the other hand dissuades the continuous building-block effect in a cyber ecosystem by attempting to negate the previous action, which leads to equilibrium, system "death," and no activity at all.[51]

Given the importance of feedback effects in a cyber ecosystem, one can achieve a continuing advantage during a cyber conflict by managing feedback effects. An increase in the negative feedback effect would lead to improved stability of the cyber ecosystem. Likewise, an increase in the positive feedback effect would lead to instability of the cyber ecosystem. On the surface, this would seem to imply that one should strive for stability over instability due to the ability to predict belligerent actions and their corresponding effects during a cyber conflict. However, the notion of predictability introduces vulnerability. In warfare, being predictable is potentially a vulnerability. The ability to manage perceptions and reactions of a designated target becomes a key facet of conflict, an assertion articulated best by Sun Tzu:

> Engage people with what they expect; it is what they are able to discern and confirms their projections. It settles them into predictable patterns of response, occupying their minds while you wait for the extraordinary moment—that which they cannot anticipate.[52]

Vulnerability arises because the belligerents in a cyber war would share a common operational picture, which could leave each side vulnerable due to their equal ability to gauge each other's actions and potential counter-actions during a cyber conflict. Thus, striving for stability and the resulting predictability goes against a fundamental principle of war—the principle of *surprise*. Since surprise is fundamentally a temporal phenomenon that results from the combination of both time and readiness, it would requires that one strike the enemy at a time,

---

[50]John Cleveland, "Complexity Theory: Basic Concepts and Application to Systems Thinking," http://www.swconnect.org/sites/default/files/Complexity_Theory_Basic_Concepts.doc.pdf (accessed 14 February 2014).

[51]Ibid.

[52]Philip Martin Mccaulay, *Sun Tzu's the Art of War* (S.l.: Lulu Com, 2009), 36.

place, or a manner for which he is unprepared in order to achieve a successful attack.[53] Conversely, the perceived ability to gauge each other's actions and employ countermeasures as appropriate could also serve as a mutual deterrent to belligerents, which give rise to the applicability of deterrence theory in cyber space.

On Mutual Cyber Deterrence

The theory of deterrence is a strategic concept focused on influencing the choices made by an adversary.[54] This is accomplished by influencing an adversary's expectations of how one would behave in response to a given action. In essence, it is concerned with discouraging an actor from acting in ways that are advantageous to them, but harmful to you.[55] Its utility as a potential operational DOD strategy in cyber space arises when belligerents in a potential cyber conflict seek the same operational strategy.

On the other hand, this could be a self-defeating endeavor because it is not decisive. A near perfect scenario, in which the belligerents in a cyber conflict have the same equal capabilities and vulnerabilities in their respective ecosystems, supports this point of view. In this instance, if the belligerents seek to optimize predictability in their respective cyber ecosystems via an increase in negative feedback effects, effectively creating a stalemate. The desired outcome of relative advantage in the infosphere becomes untenable because their actions effectively cancel out each other.

The notion of mutual deterrence as an operational theory for cyber warfare, however, offers limited utility in most cyber conflicts because it might not be decisive. This is because deterrence is a theory, which presupposes the intelligence and rationality of one's opponent.

---

[53]Robert Leonhard, "Surprise," 1-4, http://www.jhuapl.edu/ourwork/nsa/papers/surprise.pdf (accessed 3 March 2014).

[54]Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University, 1980), 9.

[55]Ibid.

However, rationality as a concept remains subjective in nature because is bounded. It depends upon the circumstances and preferences of the individual belligerents.[56] Thus the belligerents in a cyber conflict can each remain rational within their respective frameworks of understanding, whether their frameworks of understanding are similar or diametrically opposed.

TOWARDS AN OPERATIONAL THEORY FOR CYBER WARFARE

As the newest entrant into the eternal phenomenon of war, it continues to be debated whether cyber warfare qualifies as a true form of warfare. This is because pundits question the applicability of Clausewitz's definition of war to the cyber environment. They have gone as far as to say, "Code can't explode."[57] To address the ongoing discourse, the position taken in this monograph is that conflict in the cyber realm constitutes a form of warfare in the classical sense. Supporting this premise is the belief that where war is enduring in nature, warfare is subject to change. Thus, where a theory of war seeks to explain the enduring nature of war based on four continuities—a political dimension, a human dimension, the existence of uncertainty and the contest of wills—a theory of warfare, seeks to explain the constantly changing means by which one fights a war.[58]

Clausewitz defines war as an "act of force (physical force) to compel the enemy to do our will."[59] By extending this definition to the cyber realm, one can metaphorically equate cyber warfare to the "act or use of intellectual force" to compel the enemy to do one's will. This line of interpretation does not seek to deny the validity of Clausewitz definition of war, but rather seeks

---

[56]Lawrence Freedman, *Deterrence* (Cambridge, UK: Polity Press, 2004), 29.

[57]Gal Beckerman, "Is Cyber War Really War?" http://www.bostonglobe.com/ideas/2013/09/15/cyberwar-really-war/4lffEBgkf50GjqvmV1HlsO/story.html (accessed 3 March 2014).

[58]"Maneuver Self Study Program: Nature and Character of War and Warfare," http://www.benning.army.mil/mssp/Nature%20and%20Character/ (accessed 14 February 2014).

[59]Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

to extend his classical definition of war into the metaphysical digital environment. Thus, the act or use of this intellectual force leads to a "clash of intellect" between belligerents during a cyber conflict. The upper hand goes to the party with the requisite intellectual capacity to skillfully manipulate ones and zeroes in such a manner to outmaneuver the opponent. This is accomplished through superior cyber awareness and understanding.

This clash of intellect also serves to reinforce an earlier assertion that it was intellectual capital, as demonstrated by individual/organizational competence, that served as the key energy flow required to sustain the cycle of competitiveness in a given cyber ecosystem. This is because the human actor (human dimension) in the ecosystem creates the software application (application dimension) using a programming language, which is executed on a platform (infrastructure dimension) of the cyber ecosystem in "ones and zeroes." This dialect of "ones and zeroes" serves as the fundamental micro-level means through which human-instructions are interpreted by a computer-based system and executed.

Furthermore, besides the interpretations drawn above, an international group of independent experts recently reached a consensus that cyber operations constitute a use of force.[60] Key to their proposition was an acknowledgement that while cyber warfare might lack a clear kinetic parallel, a cyber operation constituted a use of force as long as the scale and effects were comparable to non-cyber operations rising to the level of a use of force.[61] An act (e.g., cyber attack) need not have immediate physical consequences to comprise a use of force, although

[60]Michael Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal* 54 (December 2012): 19, http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf (accessed 3 March 2014).

[61]Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," 19-20.

determining a "threshold" for the use of force in cases not involving physical harm presented a dilemma.[62]

Given these interpretations and understanding, there is a consensus around the idea that cyber warfare is a form of war within the broader phenomenon of war. Essentially, it is a conflict conducted within the infosphere with the aim of influencing the will and decision-making capability of the enemy in the theater of *Computer Network Operations*; attacks against this network through ones and zeroes constitute a cyber attack.[63]

For a cyber attack to occur, three conditions must be present: 1) an opponent's vulnerability, 2) attacker's access to the vulnerability, and 3) attacker's capability to exploit the vulnerability. The capability to exploit the vulnerability typically comes in one of two forms depending on the pattern of exploitation: targeted attacks or opportunistic attacks.[64] Targeted attacks are directed against specific users or organizations, and normally employ a combination of tools or techniques to accomplish the attacker's objectives. Opportunistic attacks on the other hand, are much more random in nature and rely on the element of "luck" as a key element of its attack strategy. In this case, potential victims are randomly targeted en-mass with the hope that a subset of the victims would fall prey to the attack vector.

Both state and non-state actors alike, driven by a combination of intrinsic and extrinsic motivations, perpetrate both forms of attack. Furthermore, both types of attacks could be *multi-stage* in character. For example, *computer A* penetrates *computer B* to use as a platform for

---

[62]Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," 20.

[63]Fred Schreier, "On Cyber warfare." DCAF Horizon 2015 Working Paper No. 7, 25, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCwQFjAB&url=http%3A%2F%2Fwww.dcaf.ch%2Fcontent%2Fdownload%2F67316%2F1025687%2Ffile%2FOnCyberwarfareSchreier.pdf&ei=sVcVU_D9JcShrgHi5YDoBA&usg=AFQjCNHSti4VD11zqhHbyC36ASV-0RLJ8g&bvm=bv.6 (accessed 3 March 2014).

[64]Kshetri, "Pattern of Global Cyber War and Crime: A Conceptual Framework.", 541-62.

penetrating *computer C*, which is then used to attack *computer D*.[65] It is the combination of these issues that results in the often-mentioned attribution problem. The nature of the attribution problem is such that it is often difficult, if not near-impossible, to determine with certainty who an attacker is or if actors in cyberspace are operating independently or in support of a state-sanctioned activity; a factor amplified by the relative anonymity that cyberspace offers.

Thus, nation-states have an avenue for espousing a stance of plausible deniability, even though they might be active, albeit clandestine, proponents of cyber attacks against potential adversaries. However, the reality is that given a sufficient amount of time and the right type of tools, it is possible to trace the physical origins of every cyber attack because every cyber attack leaves a digital footprint. When traced, if the attack cannot be directly linked to a state-sanctioned activity, it is typically lumped into the category of cyber crime and passed on to law enforcement agencies who typically attempt to pursue legal action. The issue with this approach is it fails to acknowledge that, just as in normal everyday social interactions, there could potentially be different dramaturgical perspectives at play in cyberspace.

War and crime are not totally disjointed phenomena. Although they have crucial differences—war is usually conceived as a group action, whereas crime is an individual one—they are cognitively linked.[66] This is because war is fundamentally a legalized crime and crime is war-like activity conducted outside of a governing legal framework. The strict relationship

---

[65]David Clark and Susan Landau, "Untangling Attribution," *Harvard Law School National Security Journal* (16 March 2011): 1, http://harvardnsj.org/wp-content/uploads/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf (accessed 13 February 2014).

[66]Teresa Degenhard "Between War and Crime: The Overlap between War and Crime: Unpacking Foucault and Agamben's Studies within the Context of the War on Terror," *Journal of Theoretical and Philosophical Criminology* 5, no. 2 (2013): 31-32, http://www.jtpcrim.org/July-2013/Article-2-Revision-for-Foucault-and-Agamben-Degenhardt-July-2013.pdf (accessed 5 April 2014).

between war and crime is apparent, especially in relation to the use of the metaphor, "war against crime," in political campaigns.[67]

As a theory of behavior, dramaturgy suggests that identity is not a stable and independent psychological entity. This is because as the person interacts with others, that person is constantly remaking their identity, leading to two different narratives—a front stage and backstage narrative. Thus, in cyberspace, since an actor's identity is not a stable and independent psychological entity, potential acts of war against the civilian private sector could potentially be mis-categorized as a cybercrime, and automatically placed under civilian criminal jurisprudence for resolution rather than deducing the real cyber intent.

This is a reflection of the troubling tendency to treat cyber warfare and cyber crime as mutually exclusive events and a failure to recognize that it is possible to have a criminal dimension to a cyber conflict. Efforts must be made to draw corollaries between perceived incidents of cyber crime to determine what the overall *cyber intent* is and whether or not it constitutes an act of war. The efforts should focus on deducing the true cyber intent of targeted attacks against the public and private sector entities.

DOD can also achieve greater operational synergies by adopting a perspective in which cyberspace is viewed as an open-system within an infosphere because it would facilitate the integration of technological based warfare. Current DOD doctrine divides technological based warfare into two distinct forms of warfare: Electronic Warfare (EW) and Cyber Warfare (CW). Current DOD doctrine defines EW as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.[68] DOD doctrine

---

[67]Degenhard "Between War and Crime: The Overlap between War and Crime: Unpacking Foucault and Agamben's Studies within the Context of the War on Terror.", 34.

[68]US Department of Defense, *Electronic Warfare*, Joint Publication 3-13, I-2 (Washington, DC: US Government Printing Office, 25 January 2007).

also defines CW as military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict.[69]

Where EW focuses on electronic attack, electronic protection, and electronic warfare support, CW focuses on cyber attack, cyber defense, and cyber enabling actions. However, there are operational concerns across both forms of warfare, which complement each other and can be used to overcome their individual limitations.

A perfect example of the synergies, herein dubbed the "access-proximity" solution, occurs when EW capabilities are used to solve CW-related issues of proximity; likewise, CW is used to solve EW-related issues of access. When these synergies are fully exploited, EW capabilities may serve as a means of accessing otherwise inaccessible networks to conduct cyberspace operations, presenting new opportunities for offensive action as well as the need for defensive preparations.[70] This is because EW does not have an access problem, since directed energy can either destroy or control anything in its path. Rather it has a proximity problem due to the possibility of the obstruction or interference with the directed energy. On the other hand, CW does not have a proximity problem. It has an access problem because the successful prosecution of an attack is predicated on the existence of vulnerability in a given cyber ecosystem. Therefore, by leveraging the respective strengths of each of these forms of warfare, one can overcome their individual limitations. This leads to the conceptualization of *Cyber-Electro* warfare as a new form of warfare. .

While there is a growing recognition across the Unites States military services of the relationship between the cyberspace and the EMS, this recognition stems purely from operational

---

[69]US Department of Defense, Joint Chiefs of Staff, *Joint Terminology for Cyberspace Operations*, by James E. Cartwright, Memorandum, 8 (Washington, DC: 2010).

[70]US Government Accountability Office, GAO-12-479, *Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight*, (Washington, DC: July 2012), 27.

necessity rather than an ontological understanding of cyberspace. This assertion hinges on the premise that the DOD definition of cyberspace remains fundamentally flawed because cyberspace is a complex adaptive ecosystem, not a domain onto itself. By treating it as a domain, the holistic value of information in the infosphere is undermined.

To overcome the potential stalemate effect associated with mutual deterrence, the operational art element of *tempo* becomes central. Tempo is a crucial element of *maneuver* warfare that relies on speed and surprise to attack an enemy's cyber ecosystem. [71] Tempo dictates the relative speed and rhythm of offensive and defensive cyber operations over time with respect to the enemy.[72] The need for surprise stems from a desire to circumvent a problem and attack it from a position of advantage rather than meet it straight on.[73] Therefore, as in other forms of warfare, tempo is valuable in cyber warfare.

Victory in a competitive decision cycle requires one side to understand what is happening and being able to act faster than the other.[74] This axiom is the very essence of John Boyd's theory in which he recognizes the need to cycle through a mental model—observe, orient, decide, act (OODA) loop—at a pace much faster than the enemy.[75] Thus in cyber warfare, operational success would be dependent on *speed* with the upper hand going to the party with the greater ability to act or react faster in the highly complex cyber ecosystem.

---

[71]US Navy, USMC Doctrine Reference Publication, MCDP 1, *Warfighting* (Washington, DC, 20 June 1997), 38-40.

[72]US Army, ADRP 3-0, *Unified Land Operations,* Army Doctrine Reference Publication (Washington, DC, May 2012), 55.

[73]US Navy, *Warfighting,* 38-40.

[74]Scott Applegate, "The Principle of Maneuver in Cyber Operations", 185 (2012 4th International Conference on Cyber Conflict, NATO CCD COE Tallinn, 2012).

[75]Frans Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd, 2,* (Delft: Eburon Academic Publishers, 2005).

Furthermore, given the limitations of deterrence as a possible operational theory for cyber warfare it is proposed that, rather than seeking to optimize predictability in a given cyber ecosystem by increasing the negative feedback effect, the opposite is in fact more desirable. By decreasing the predictability of one's cyber ecosystem, one is able to reduce the vulnerability picture. Thus, the stability and resulting predictability of one's own cyber ecosystem can decrease by increasing the positive feedback effect.

Decreased understanding is akin to the introduction of "fog" into one's own ecosystem in order to mitigate the adversary's ability to predict an outcome and thus respond preemptively. In this regard, *cyber decoys* can be employed as a classical form of deception to introduce fog from an adversary's perspective. Under this paradigm, decoy rules, developed and integrated into the daily operations of the organization, guide actors within each of the dimensions of a cyber ecosystem. The problem with this approach, however, is that one must take care to ensure the use of cyber decoys does not rise to the level of perfidy, the treacherous misleading of an enemy about his—or your—status under the law."[76]

Thus, to decrease the stability and resulting predictability of one's own cyber ecosystem, one should seek to increase the positive feedback effects. The increase in positive feedback effects would, in turn, introduce *chaoplexity* into the cyber ecosystem—a neologic term created out of an amalgamation of chaos and complexity theory.[77] Moreover, it is through this phenomenon that a can one can deduce a semblance of coherence in the midst of chaos and complexity.

---

[76]Michael Brett and Thomas Wingfield, "Lawful Cyber Decoy Policy" (International Federation for Information Processing, 8th International Conference on Information Security, Athens, Greece, May, 2003), 4, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.108.7169&rep=rep1&type=pdf (accessed 3 March 2014).

[77]Antoine Bousquet, "Chaoplexic Warfare or the Future of Military Organization," *International Affairs* 84, no. 5 (September 2008): 923, doi:10.1111/inta.2008.84.issue-5 (accessed 15 February 2014).

Managing the Positive Feedback Effect

As a rule of thumb, a cyber ecosystem is deterministic in nature by virtue of the antecedent impact of both positive and negative feedback effects. The central tenet of chaoplexity is that it is at the point of instability that order emerges from chaos. Chaoplexity is the resulting behavior when chaos presents the possibility of order rather than a threat to order.[78]

The emergence of chaoplexity in the cyber ecosystem shifts the focus from the traditional approach of the stabilization and self-regulation of an ecosystem based on the management of negative feedback effects to the exploitation of the positive feedback effect that leads to the emergence of chaoplexic behavior.[79] Its utility to the current discourse stems from the fact that the most successful "systems" are those that retain flexibility and openness in the interaction and organization of their parts within environments, while at the same time eluding complete predictability. [80] Since the resulting chaoplexic behavior in the cyber ecosystem is not random, it must be managed. The ability to manage the chaoplexic behavior in the cyber ecosystem is achieved by identifying and managing the state of the key dimensions, which drive the dynamics of the whole cyber ecosystem.

The identification of the key dimensions is accomplished by classifying each dimension of the cyber ecosystem into one of three possible categories based on the predominant role, which it plays in a cyber ecosystem. These categories are: critical, meaning that the dimension must always be in place in order for the cyber ecosystem to function; redundant, meaning that it is never required for the ecosystem to function; and intermittent, meaning that it acts as driver dimension in some or all parts of the ecosystem.[81]

---

[78]Bousquet, "Chaoplexic Warfare or the Future of Military Organization," 915-29.

[79]Ibid.

[80]Ibid.

[81]Tao Jia et al., "Emergence of Bimodality in Controlling Complex Networks," *Nature*

In this regard, the key dimension is the human dimension, which drives the dynamics of the whole cyber ecosystem. This is because the energy flow of intellectual capital manifests itself in a cyber ecosystem. Recognizing the human dimension as the key dimension to manage chaoplexic behavior leads to the identification of two potential approaches: centralized and distributed management.[82]

In a centralized approach towards managing chaoplexity, one can achieve control of their cyber ecosystem through a small fraction of all the dimensions specific to their organization. A distributed approach towards managing chaoplexity requires the distribution and sharing of responsibility. The obvious consequence of a centralized approach is that an organization, in this case DOD, can only focus on the security of its own cyber ecosystem because a distributed approach will require significant resources. More importantly, legal constraints pose a barrier to DOD's ability to manage the cyber ecosystem of organizations in the civilian private sector. Thus, a distributed approach towards managing chaoplexity is required, and this approach should encompass the civilian private sector. The question now arises: what does this mean for cyber warfare?

Operational Implications

The overall implication of depicting cyberspace as a complex, adaptive ecosystem rather than a domain is that it provides an avenue for further understanding of the complexities associated with operating in cyberspace. It is preferable to manipulate the positive feedback effect instead of maximizing the negative feedback effect because it would introduce chaoplexity into one's cyber ecosystem. The adoption of a distributed approach towards managing chaoplexity in the cyber ecosystem requires the acknowledgement that the civilian private sector also has a

---

Communications 4 (18 June 2013): 4, DOI: 10.1038/ncomms3002 (accessed 3 April 2014).

[82] Jia et al., "Emergence of Bimodality in Controlling Complex Networks," 2.

prominent role to play in cyberspace because DOD relies on infrastructure provided by the private sector. Since the DOD cannot segregate its cyber ecosystem from the private sector infrastructure, it must resort to a constant increase of its cyber security posture to counter emerging threats. This is a defensive approach towards operating in cyberspace.

This brings to the forefront the concern raised about the current US approach to protecting its computer systems as being "too predictable," a concern raised in 2011 by the former Vice Chairman of the US Joint Chiefs of Staff, General Cartwright.[83] Specifically his concern was that the U.S approach is purely defensive with no penalty attached for attacking the U.S, and this needed to change.[84] When the status quo of emphasizing defense is viewed within the context of a nominal cyber aggressor, such as China, arguments can be made that engaging in a defensive stance is exactly what China wants the United States to do. This is because the Chinese approach towards strategy depends on the enticement of technologically superior opponents into unwittingly adopting a strategy that will lead to their defeat.[85]

This approach is highlighted in the works of Li Bingyan, one of the most influential and brilliant contemporary Chinese strategists, in which he provides a perfect analogy of how this is accomplished. Using the example of a weak mouse (i.e., China) trying to keep track of a huge cat (i.e., the United States), he asks, "How could a mouse hang a bell around a cat's neck?" His answer: "The mouse cannot do this alone or with others. Therefore, the mouse must entice the cat to put the bell on himself."[86]

---

[83]Ellen Nakashima, "US Cyber Approach 'Too Predictable' for One Top General," *Washington Post*, (14 July 2011) http://www.washingtonpost.com/national/national-security/us-cyber-approach-too-predictable-for-one-top-general/2011/07/14/gIQAYJC6EI_story.html (accessed 23 March 2014).

[84]Ibid.

[85]Attributed to Li Bingyan, *Applying Military Strategy in the Age of the New Revolution in Military Affairs*, by Timothy L. Thomas, "The Chinese Military Strategic Mindset," *Military Review* 47 (Nov-Dec 2007), http://fmso.leavenworth.army.mil/documents/chinese-mind-set.pdf.

[86]Timothy L. Thomas, "The Chinese Military Strategic Mindset," *Military Review*, 47 (Nov-Dec

Essentially, what is happening is that it is very plausible that China has deliberately sought to foster the creation of a flawed US narrative for operating in cyberspace—a narrative that emphasizes cyber security. Public record accounts attribute most cyber attacks against USG, as well as private sector-owned computer systems, to the Chinese government, and the military supports this assertion.[87] This observation is critical because it illustrates China's emphasis of the indirect approach towards gaining the upper hand. This indirect approach typifies the Chinese stratagem of deception.

Precision as an Operational Art Element in Cyberspace Operations

The ability to successfully manage the positive feedback effects suggest that a new operational art element specific to the cyber realm would apply—the operational art element of precision. Delivering precision effects is the intended outcome of offensive operations.[88] For conventional kinetic weapons, precision effects are synonymous with low-collateral damage. In cyber operations, operators typically rely on intuitive estimates, which depend in large part on the experience and expertise of the operator. Given the heavy reliance on intuition, the need for intellectual capital development remains critical. Furthermore, since it is impossible to know precisely the future of any phenomena, except the probabilities that lay ahead, the focus of effort in ensuring precision as is to increase probabilistic confidence levels during cyberspace operations.[89]

—

2007), http://fmso.leavenworth.army.mil/documents/chinese-mind-set.pdf (accessed 3 April 2014).

[87]US Office of the Secretary Of Defense, *Military and Security Developments Involving the People's Republic of China 201 3: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2000*, 113th Cong., Report (Washington, DC, 2013).

[88]Kamal Jabbour, "The Science and Technology of Cyber Operations" (Air, Space, and Cyberspace Power in the 21st Century 38th IFPA-Fletcher Conference on National Security Strategy and Policy, 20 January 2010), http://www.ifpafletcherconference.com/2010/transcripts/session4_Jabbour.pdf (accessed 5 April 2014).

[89]Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age*,

US Policy Implications

The current integration of USG assets with civilian systems makes segregation impossible and creates a responsibility for the US to protect those civilian networks, services, and communications.[90] To accomplish this, the USG has largely adopted cyber security as a key theme of its undeclared and unofficial policy for operating in cyberspace. Although inextricably linked, cyber security and cyber warfare represent two somewhat opposing concepts. Where cyber security is primarily defensive in nature, cyber warfare is both offensive and defensive in nature. The crosscutting concern for both cyber security and warfare is "defense." It is only logical the emphasis of the USG official policy position would center on a defensive approach towards operating in cyberspace. The current efforts, although necessary and beneficial, attempt to increase the negative feedback effect in order to make the US cyber infrastructure more resilient to cyber attacks. The implications of this approach require a never-ending cycle of building in mechanisms to protect its cyber infrastructure.

To develop a more plausible narrative for operating in cyberspace, the US must switch focus. In order to do this it need not look any further than the old adage, which states that the best form of defense is attack. This suggests that adopting a policy position that is primarily offensive in nature better serves the US, especially in regards to the protection of the cyber ecosystems of the private sector. The fact that most, if not all, of the underlying infrastructure for seamless cyber interactions are controlled and managed by non-state entities means that the USG most recognize the power of the private sector in cyberspace.[91] Simply put, offensive cyber attacks should not be limited to only the authorized entities of the United States military. Excerpts from a paper

---

Vol. 6 of Cass Series-Strategy and History (London: Frank Cass, 2005), 101.

[90]Jensen, "Cyber Warfare and Precautions against the Effects of Attacks."

[91]Choucri and Clark, "Cyberspace and International Relations towards an Integrated System," 33.

presented to the Judiciary Committee's Subcommittee on Crime and Terrorism further emphasizes this position. In the paper, the author Stewart A. Baker, a partner of Steptoe & Johnson LLP, described the actual defensive approach of cyber security with following metaphor:

> We are not likely going to defend our way out of this problem. . . . In short, we can't defend our way out of this fix, any more than we could solve the problem of street crime by firing our police and making pedestrians buy better body armor every year. . . . I'm not calling for vigilantism, I'm not calling for lynch mobs. But we need to find a way to give the firms doing these investigations authority to go beyond their network. . . . If we don't do that we will never get to the bottom of most of these attacks."[92]

Such an offensive minded policy, if adopted, would enable the application of special offensive techniques to mitigate cyber threats such as the use of intrusive malware to track intruders or malicious code to spread in targeted "spear-phishing" campaigns against those actors suspected to have originated the offensive action.[93]

The use of such malware could neutralize cyber attacks and gather a huge quantity of information from the systems attacked. One can use this information to profile the attackers and prevent future attacks.[94] The same data can also be used to deliberately introduce "fog" (manageable positive feedback effects) into one's cyber ecosystem by deliberately preventing infection of those systems that have a high probability to be exploited by the same attackers in future offensives.

The proposed policy option comes with an acknowledgment of the potential legal implications, as it requires the promulgation of appropriate laws to regulate such offensive action. When weighed within the context of the status quo, the adoption of this policy option would shift the debate from perfect attribution to accountability. It would, however, require the

---

[92]Paganini, "The Offensive Approach to Cybersecurity, Motivations and Risks."

[93]Paganini, "The Offensive Approach to Cyber Security in Government and Private Industry."

[94]Ibid.

acknowledgement of the operational art element of precision to guard against unintended consequences.

Operating in cyberspace requires a collaborative effort rather than placing the preponderance of responsibility for protecting cyberspace on DOD. Hostile actors in cyberspace as well as would be attackers remain comforted by the fact that the DOD will not respond in kind to cyber attacks against civilian private sector entities. Cyber attacks against such entities are treated as cyber crimes by a law enforcement framework. However, the chances for conviction remain slim for attackers located outside the United States, given the poor record of the Budapest Cybercrime Convention.

CONCLUSION

Cyberspace has created a new reality that is a source of vulnerability, a potential threat to national security, and a disturber of the familiar international order.[95] Essentially, the intermixing of public and private infrastructure and the reliance of the US government on private infrastructure makes cyberspace a complex environment because the major actor that constitutes and defines international relations—the state—is not able to control cyberspace or insulate itself from the implications of the new cyber realities.[96]

This represents an unmistakable challenge to national security, because cyber threats have the potential to be indiscriminate in nature, and the current integration of US Government assets with civilian systems makes segregation impossible. The resulting implication is the lack of a clear distinction between cyber attacks that constitute acts of war and those that constitute criminal activities. Furthermore, as a non-state actor, the private sector is largely rendered helpless and must rely on defensive mechanisms to protect itself from cyber attacks due to the

[95]Choucri and Clark, 2.

[96]Ibid.

legal prohibition on launching offensive-styled counter-attacks. Hence, operating in cyberspace remains a challenge, due to the complexity of the underlying architectural framework and legal constraints that restrict offensive activities of non-state actors.

This a situation amplified by the failure to correctly establish whether we are confronted by an MR or an RMA, a failure which carries significant policy implications. This is because although the concept of MR and RMAs are primarily intellectual constructs, they both have value, as the correct selection would help shed light on an appropriate policy option for the USG.[97] The prevailing view of cyberspace as a domain, and a closed system reflects the human preference to exercise a form of analytical simplification to control cyberspace. However, it is impossible to control an open system. At best, one can manage an open system. Moreover, the DOD does not have the legal authority to manage the infrastructure owned and operated by organizations in the civilian private sector. This presents a powerful challenge to traditional theory and practice that cyberspace, with its ubiquity and global reach, be managed by private sector entities[98]

Furthermore, the anonymity problem and the resulting attribution issues, made possible by flaws in the design of the Internet, introduce vulnerabilities into the cyber ecosystem. When these flaws are exploited, what initially appeared to be a seemingly innocuous vulnerability could quickly lead to a breach of the integrity of one's cyber environment. It is the prevalence of these flaws that led the former NSA Director, Mike McConnell, to suggest that the Internet needed to be reengineered to make attribution, geo-location, intelligence analysis, and impact assessment—i.e., who did it, from where, why, and what was the result—more manageable.[99] His assertion,

---

[97]Colin S. Gray, *Cass Series. Strategy and History*, vol. 2, *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History* (London: Frank Cass, 2004), 31.

[98]Choucri and Clark, 33.

[99]Mike McConnell, "Mike McConnell on How to Win the Cyber-War We're Losing," *Washington*

although valid, asks an unanswerable question: Who should have primary responsibility for reengineering the Internet? Given the fact that this is not going to occur any time soon, a paradigm shift is required for operating in cyberspace. In this regard, cyberspace should be conceived as a complex adaptive system consisting of three key dimensions: the human, application and infrastructure dimension.

The blatant omission of the human dimension in the current definition diminishes the role of the most important actor in the information loop. The focus of thought and action then shifts from the creation and prevention of operational effects to the arena of traditional war fighting concepts.[100] Thus traditional war fighting concepts such as control, maneuver, and superiority, etc., become the priority of effort at the expense of investing appropriately in the requisite human capital needed to employ the traditional war fighting concepts.[101]

Although innovation plays a role, the ability of a state to cope with increasing complex battlefields is the true determinant of success.[102] Since cyberspace is inherently a dynamic, complex adaptive ecosystem, its complexity would only increase with advances in technology. Given the introduction of positive feedback effects, the traditional linkage of ways and means to the achievement of discrete ends is disrupted.[103] This is because, although ways and means may be deployed in cyberspace with the best of intentions, the resulting outcomes could potentially be

---

Post, Sunday, 28 February 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (accessed 13 February 2014).

[100]Libicki, "Cyberspace Is Not a Warfighting Domain.", 328.

[101]Ibid.

[102]Gray, *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*, 31.

[103]Stevens, "UK Cyber Security: Grand Strategy and the State."

unexpected and in some cases counter-productive.[104] Thus, efforts must be made to control the positive feedback effect.

A perfect example of how things can go awry if not managed properly is best exemplified by the 2008 cyber attack initiated by the US military against a Saudi-CIA "honeypot." The honeypot was initially set up as an online forum, covertly monitored by intelligence agencies to identify attackers and gain information; and yield information, it did. However, with growing concern by the US military that the site was being used to pass operational information among extremists, a decision was made to "shut it down." When the site was eventually shut down, the unintended consequence was the inadvertent disruption of more than 300 servers in Saudi Arabia, Germany, and Texas.[105]

Since the infosphere is the only domain in which all instruments of national power—diplomatic, informational, military, and economic—is concurrently exercised through the manipulation of data and gateways, it holds that this domain must be aggressively protected. [106] In this regard, the adoption of a policy position, which is primarily offensive in nature, would offer greater utility over a defensive policy because, in the parlance of strategic analysis, offensive action is easier, quicker, and usually cheaper than defensive action.[107] This policy position should cover both DOD and the private sector entities, and pave the way for development of the requisite intellectual capital needed to prosecute such activities. In this regard, the focus of the US university educational system must change because, of over forty-eight universities designated as cyber security Centers of Academic Excellence–Research (CAE-R) by the N.S.A., only five are actively researching offensive and defensive cyber operations to a

[104]Stevens, "UK Cyber Security: Grand Strategy and the State."

[105]Nakashima, "Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyber war Policies," *Washington Post*.

[106]Schreier, "On Cyberwarfare."

[107]Ibid.

broader extent.[108] Essentially, this means a vast number of US academic institutions are unable as of today to look at and conduct research beyond information security that is incompatible with an offensive minded culture.[109]

Lastly, while history has shown that it is ambitious to expect all countries to agree on anything, the nature of cyberspace is such that a specific declaratory offensive US policy would generate a response, placing the burden on states to take a more aggressive stance on transnational cyber criminal activities.

[108]Kallberg and Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority," 55 -56.

[109]Ibid.

BIBLIOGRAPHY

Adams, Colin Conrad, and Robert David Franzosa. *Introduction to Topology: Pure and Applied*. Upper Saddle River, NJ: Pearson Prentice Hall. 2008.

Applegate, Scott. "The Principle of Maneuver in Cyber Operations." 2012 4th International Conference on Cyber Conflict. NATO CCD COE Tallinn. 2012.

Ammann, Eckhard. "A Hierarchical Modelling Approach to Intellectual Capital Development." *The Electronic Journal of Knowledge Management* 8, no. 2 181-91.

Delgado, Jaime Barrientos, Paulina Salinas Meruane, Pablo Rojas Varas, and Patricio Meza Opazo. "Gender Relations and Masculinity in Northern Chile Mining Areas: Ethnography in Schoperías." http://www.scielo.gpeari.mctes.pt/pdf/etn/v15n3/v15n3a01.pdf (accessed 30 March 2014).

Beckerman, Gal. "Is Cyberwar Really War?" http://www.bostonglobe.com/ideas/2013/09/15/cyberwar-really-war/4lffEBgkf50GjqvmV1HlsO/story.html (accessed 3 March 2014).

Berkes, Fikret, Johan Colding, and Carl Folke, eds. *Navigating Social-Ecological Systems: Building Resilience for Complexity and Change*. Cambridge: Cambridge University Press, 2003. http://0-dx.doi.org.oasis.unisa.ac.za/10.1017/cbo 9780511541957 (accessed 10 April 2014).

Bingyan, Li. "Applying Military Strategy in the Age of the New Revolution Military Affairs." *The Chinese Revolution in Military Affairs*. Edited by Shen Weiguang. China: New China Press, 2004.

Bousquet, Antoine. "Chaoplexic warfare or the future of military organization." *International Affairs* 84, no. 5 (September 2008): 915-29. doi:10.1111/inta.2008.84.issue-5 (accessed 15 February 2014).

Brett, Michael and Thomas Wingfield. "Lawful Cyber Decoy Policy." International Federation for Information Processing, 8th International Conference on Information Security. Athens, Greece. May 2003. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.108.7169&rep=rep1&type=pdf (accessed 3 March 2014).

Chapin, F. Stuart, P. A. Matson and Harold A. Mooney, *Principles of Terrestrial Ecosystem Ecology* (New York: Springer, 2002).

Choucri, Nazli and David Clark. "Cyberspace and International Relations toward an Integrated System." *Explorations in Cyber International Relations* 8, no. 25 (August 2011): 1. http://ecir.mit.edu/images/stories/Salience%20of%20Cyberspace%208-25.pdf (accessed 23 March 2014).

Clark, David and Susan Landau. "Untangling Attribution." *Harvard Law School National Security Journal* (16 March 2011): 1. http://harvardnsj.org/wp-content/uploads/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf (accessed 13 February 2014).

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco, 2010.

Clausewitz, Carl von. *On War*. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Cleveland, John. "Complexity Theory: Basic Concepts and Application to Systems Thinking." http://www.swconnect.org/sites/default/files/Complexity_Theory_Basic_Concepts.doc.pdf (accessed 14 February 2014).

Council of Europe "Convention On Cybercrime CETS No.: 185." Council of Europe. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (accessed 14 February 2014).

Conca, K. "Rethinking the Ecology-Sovereignty Debate." *Millennium—Journal of International Studies* 23, no. 3 (March 1994): 701-11. Doi:10.1177/03058298940230030201 (accessed 14 February 2014).

Degenhard, Teresa. "Between War and Crime: The Overlap between War and Crime: Unpacking Foucault and Agamben's Studies with in the Context of the War on Terror." *Journal of Theoretical and Philosophical Criminology* 5, no. 2 (2013): 29-58. http://www.jtpcrim.org/July-2013/Article-2-Revision-for-Foucault-and-Agamben-Degenhardt-July-2013.pdf (accessed 5 April 2014).

Dolman, Everett C. *Pure Strategy: Power and Principle in the Space and Information Age*. Vol. 6 of *Cass Series—Strategy and History*. London: Frank Cass, 2005.

"Environmental Biology—Ecosystems." http://www.marietta.edu/~biol/102/ecosystem.html#Energyflowthroughtheecosystem3 (accessed 14 February 2014).

"Food Web Background." http://www.seagrant.sunysb.edu/ifishny/pdfs/lessons/inclass/elementary/FoodWeb-Background.pdf (accessed 3 April 2014).

Franzese, Lieutenant Colonel Patrick W. "Sovereignty in Cyberspace: Can It Exist?" *The Air Force Law Review, AFPAM 51-106* 64 (2009).

Freedman, Lawrence. *Deterrence*. Cambridge, UK: Polity Press, 2004.

Ghosh, Sumit, and Elliot Turrini. *Cybercrimes: A Multidisciplinary Analysis*. Berlin: Springer, 2010.

Glaser, Marion, Gesche Krause, Beate Ratter, and Martin Welp. "Human / Nature Interaction in the Anthropocene Potential of Social-Ecological Systems Analysis." http://www.dg-humanoekologie.de/pdf/DGH-Mitteilungen/GAIA200801_77_80.pdf (accessed 30 March 2014).

Gray, Colin S. *Cass Series. Strategy and History*. Vol. 2, *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*. London: Frank Cass, 2004.

Holl, Kim. “OSI Defense in Depth to Increase Application Security.http: //www.giac.org/paper/gsec/2868/osi-defense-in-depth-increase-application-security/104841 (accessed 14 February 2014).

“Important Scientists: Erwin Schrodinger (1887–1961).” *The Physics of the Universe.* http://physicsoftheuniverse.com/scientists_schrodinger.html (accessed 15 February 2014).

Jabbour, Kamal. “The Science and Technology of Cyber Operations.” Air, Space, and Cyberspace Power in the 21 St Century 38th IFPA-Fletcher Conference on National Security Strategy and Policy. 20 January 2010. http://www.ifpafletcherconference.com/2010/transcripts/session4_Jabbour.pdf (accessed 5 April 2014).

Jensen, Eric. “Cyber Warfare and Precautions against the Effects of Attacks.” *Texas Law Review* 88 (1 June 2010): 1. http://ssrn.com/abstract=1661218 (accessed 3 March 2014).

Jia, Tao, Yang-Yu Liu, Endre Csóka, and Márton Pósfai. “Emergence of Bimodality in Controlling Complex Networks.” *Nature Communications* 4 (18 June 2013): 1-6. doi: 10.1038/ncomms3002 (accessed 3 April 2014).

Kallberg, Jan, and Bhavani Thuraisingham. “Cyber Operations: Bridging from Concept to Cyber Superiority.” *Joint Force Quarterly*, January. 2013. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-68.pdf (accessed 23 March 2014).

Kamhoua, C. A., and K. A. Kwia. “Survivability in Cyberspace Using Diverse Replicas: A Game-Theoretic Approach.” *Journal of Information Warfare* 12, no. 2 (23 July 2013): 1, http://www.jinfowar.com/survivability-in-cyberspace-using-diverse-replicas-a-game-theoretic-approach/ (accessed 3 April 2014).

Kellert, Stephen H. *In the Wake of Chaos: Unpredictable Order in Dynamical Systems*. Science and Its Conceptual Foundations. Chicago: University of Chicago Press, 1993.

Kshetri, Nir. “Pattern of global cyber war and crime: A conceptual framework.” *Journal of International Management* 11, no. 4 (December 2005): 541-62. doi:10.1016/j.intman.2005.09.009 (accessed 7 February 2014).

Kuhn, Thomas S. *The Structure of Scientific Revolutions*. 4th ed. Chicago: The University of Chicago Press, 2012.

Ladyman, James, James Lambert, and Karoline Wisener. “What Is a Complex System?” http://philsci-archive.pitt.edu/9044/4/LLWultimate.pdf (accessed 14 February 2014).

Leonhard, Robert. “Surprise.” http://www.jhuapl.edu/ourwork/nsa/papers/surprise.pdf (accessed 3 March 2014).

Libicki, Martin. “Cyberspace Is Not a Warfighting Domain.” *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (Fall 2012): 325-40. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf (accessed 13 February 2014).

"Maneuver Self Study Program: Nature and Character of War and Warfare." http://www.benning.army.mil/mssp/Nature%20and%20Character/ (accessed 14 February 2014).

McDowell, Stephen D., Philip E. Steinberg, and Tami K. Tomasello. *Managing the Infosphere: Governance, Technology, and Cultural Practice in Motion*. Philadelphia: Temple University Press, 2008.

Milner, Helen. "International Theories of Cooperation among Nations Cooperation Among Nations" by Joseph Grieco; Saving the Mediterranean by Peter Haas: Strengths and Weaknesses." *World Politics* 44, no. 3 (April 1992): 466-96.

Moffat, James. *Complexity Theory and Network Centric Warfare*. Information Age Transformation Series. Washington, DC: CCRP Publication Series, 2003.

Mueller, Jan-Werner. "'An Irregularity That Cannot Be Regulated': Carl Schmitt's Theory of the Partisan and the 'war On Terror'." http://www.artexetra.com/CyberneticsArtCultConv.pdf (accessed 15 February 2014).

Nash, Michele, and Lisa Rapp. "Trophic." Springfield Technical Community College. http://faculty.stcc.edu/biol102/Lectures/lesson12/trophicstruc.htm (accessed 14 February 2014).

Office of the President of the United States of America. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. UN. n.p.:Washington, DC, 2011.

Osinga, Frans. *Science, Strategy and War: The Strategic Theory of John Boyd*. Delft: Eburon Academic Publishers, 2005.

Paganini, Pierluigi. "The Offensive Approach to Cyber Security in Government and Private Industry." *Infosec Security*, 18 July 2013. http://resources.infosecinstitute.com/the-offensive-approach-to-cyber-security-in-government-and-private-industry/ (accessed 23 March 2014).

Paganini, Pierluigi. "The Offensive Approach to Cybersecurity, Motivations and Risks." http://securityaffairs.co/wordpress/14330/security/offensive-approach-cybersecurity-risks.html (accessed 5 April 2014).

Prajith, P. "Phase Space Features for Speech Modeling." http://shodhganga.inflibnet.ac.in/bitstream/10603/3960/14/14_chapter%205.pdf (accessed 15 February 2014).

Phister, Paul. "Cyberspace: The Ultimate Complex Adaptive System." *The International C2 Journal* 4, no. 2 (2010–2011): 1. http://www.DODccrp.org/files/IC2J_v4n2_03_Phister.pdf (accessed 14 February 2014).

Philip Martin Mccaulay. *Sun Tzu's the Art of War*. S.l.: Lulu Com, 2009.

Redman, C., M. J. Grove, and L. Kuby. "Integrating Social Science into the Long Term Ecological Research (LTER) Network: Social Dimensions of Ecological Change and Ecological Dimensions of Social Change." *Ecosystems*7 no 2: 161-171.

Schelling, Thomas C. *The Strategy of Conflict.* Cambridge, MA: Harvard University, 1980.

Schmitt, Michael "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard International Law Journal* 54 (December 2012): 13-15. http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf (accessed 3 March 2014).

Schreier, Fred. "On Cyberwarfare." DCAF Horizon 2015 Working Paper No. 7. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCwQFjAB&url=http%3A%2F%2Fwww.dcaf.ch%2Fcontent%2Fdownload%2F67316%2F1025687%2Ffile%2FOnCyberwarfareSchreier.pdf&ei=sVcVU_D9JcShrgHi5YDoBA&usg=AFQjCNHSti4VD11zqhHbyC36ASV-0RLJ8g&bvm=bv.6 (accessed 3 March 2014).

Sloan, Elinor. "Canada and the Revolution in Military Affairs: Current Response and Future Opportunities." *Canadian Military Journal* (Autumn 2000): 7-14. http://www.journal.forces.gc.ca/vo1/no3/doc/7-14-eng.pdf (accessed 30 March 2014).

Spafford, Eugene "An Analysis of the Internet Worm." *Proceedings of the European Software Engineering Conference, Lecture Notes in Computer Science #387.* United Kingdom, September 1989. http://spaf.cerias.purdue.edu/tech-reps/823.pdf (accessed 26 February 2014).

Stevens, Tim. "UK Cyber Security: Grand Strategy and the State." *World Defense Systems* 1 (2012): 21-23. https://www.academia.edu/1499522/UK_cyber_security_Grand_strategy_and_the_state (accessed 14 February 2014).

Thomas, Timothy L. "The Chinese Military Strategic Mindset." *Military Review* 47 (Nov-Dec 2007). http://fmso.leavenworth.army.mil/documents/chinese-mind-set.pdf (accessed 3 April 2014).

Thompson, Michael. "Military Revolutions and Revolutions in Military Affairs: Accurate Descriptions of Change or Intellectual Constructs?" http://artsites.uottawa.ca/strata/doc/strata3_082-108.pdf (accessed 29 March 2014).

US Air Force. Air Force Doctrine Document. AF DD 3-12, *Cyberspace Operations*. Washington, DC, 15 July 2010.

US Army. ADP 5.0*: The Operations Process*. Army Doctrine Reference Publication. Washington, DC, Government Printing Office 2012.

—. ADRP 3-0—*Unified Land Operations*. Army Doctrine Reference Publication. Washington, DC, Government Printing Office May 2012.

US Department of Defense, Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*. Joint Doctrine. Washington, DC, 8 November 2010 (as Amended through 15 January 2014), 64.

—. Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations*. Washington, DC, 2006.

US Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Unclassified. Washington, DC, 2011.

—. *Information Operations* – Joint Publication 3-13. Doctrine. Washington, DC, 2010.

—. Joint Publication 3-13.1. *Electronic Warfare*. Washington, DC, 25 January 2007.

—. Vice Chairman, Joint Chiefs of Staff. *Joint Terminology for Cyberspace Operations*, by James E. Cartwright. Memorandum. Washington, DC, 2010.

US Government Accountability Office (GAO). GAO-12-479. *Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight*. Washington, DC, July 2012.

US Navy. USMC Doctrine Reference Publication. MCDP 1, *Warfighting*. Washington, DC, 20 June 1997.

US Office of the Secretary of Defense. Military and Security Developments Involving the People's Republic of China 201 3: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2000. 113th Cong. Report. Washington, DC, 2013.

Weaver, Warren. "Science and Complexity." *American Scientist* 36 (1948): 536-44.